SICHERHEIT UND BETRIEBLICHE EFFIZIENZ -

ES BEGINNT MIT DER SICHTBARKEIT.

omniIT
INNOVATIVE TECHNOLOGY

Die Sicherheit medizinischer Geräte ist eine tragende Säule der Sicherheitsstrategien von Organisationen im Gesundheitswesen. Sie ist schnell zum grundlegenden Ausgangspunkt für das Verständnis der zentralen Rolle geworden, die diese Geräte für die Widerstandsfähigkeit im gesamten heiklen Prozess der Gesundheitsversorgung spielen. Ein wichtiges Ergebnis der Bemühungen der Branche, sich mit diesem Thema zu befassen, ist die Erkenntnis, dass das Ökosystem der Gesundheitsgeräte viel größer ist als nur medizinische Geräte. Dies erleichtert es, alle Infrastrukturelemente und ihre Rolle bei der Sicherung des Weges eines Patienten durch das Gesundheitssystem zu berücksichtigen.

Inhaltsübersicht

Intellektuelles Eigentum schützen

IT-Infrastruktur unterstützt das Wachstum

Einführung

Im Jahr 2021 führte Armis eine Untersuchung darüber durch, wie der National Health Service (NHS) im Vereinigten Königreich (UK) dieses Thema angeht und wie effektiv seine Strategie in den einzelnen Trusts ist. Dieses Papier bietet Leitlinien und Best Practices und gibt einen Einblick in die Forschungsergebnisse, um Gesundheitsdienstleister bei der Planung des nächsten Kapitels in diesem sich entwickelnden Bereich der Informationssicherheit und organisatorischen Widerstandsfähigkeit zu unterstützen.

UMWANDLUNG REGULATORISCHER ANFORDERUNGEN IN STRATEGISCHE PRIORITÄTEN

Unabhängig von der Art und dem Standort des Gesundheitsdienstleisters ist die Belastung durch Vorschriften weit verbreitet. Oft gibt es zwei bis sieben gesetzliche Vorschriften und Technologiestandards, die für die Gesundheits-IT und die Informationssicherheit gelten, mit sich überschneidenden Anforderungen, Zertifizierungskriterien, Zeitplänen für die Einhaltung und Strafen bei Nichteinhaltung. Im Falle des NHS hatten über 70 Trusts im Forschungspool Anforderungen, die von der Richtlinie für Netze und Informationssysteme (NIS) über Cyber Essentials und ISO 27001 bis hin zur Teilnahme am Data Security & Protection Toolkit (DSPT) als Selbstbescheinigungsinstrument reichten.

Es gibt Parallelen zu Verordnungen wie HIPAA und HITECH in den Vereinigten Staaten von Amerika (USA), den von der französischen Datenschutzbehörde erlassenen Datenschutzbestimmungen, der GDPR in der Europäischen Union (EU) und dem Gesundheitsdatengesetz für Gesundheitseinrichtungen in den Vereinigten Arabischen Emiraten (VAE). In jedem dieser Gesetze findet sich eine weitreichende Ausrichtung auf die Grundprinzipien der Informationssicherheit. Speziell in Bezug auf:

- Kontinuierliches Risikomanagement
- Organisatorischer Kontext des Sicherheitsrisikos für die Patientensicherheit
- Schwerpunkt auf dem Schutz der Privatsphäre und der Sicherheit vertraulicher Informationen über klinische und demografische Daten der Patienten
- Anforderungen für den Nachweis der betrieblichen Befähigung
- Einrichtung eines auf Standards basierenden Datenaustauschs für Sicherheitsinformationen und die Reaktion auf Zwischenfälle

Diese Anforderungen entwickeln sich jedes Jahr als Reaktion auf die sich verändernde Bedrohungslandschaft und die Innovationen im Bereich der IT im Gesundheitswesen und deren Abhängigkeit von Gesundheitsanwendungen und integrierten Daten aus medizinischen Geräten, die zur Unterstützung des klinischen Entscheidungsprozesses verwendet werden. Für Gesundheitssysteme und Krankenhäuser findet eine Konvergenz statt, die das Risikomanagement der Informationssicherheit als Funktion des Risikomanagements im Unternehmen mit der Verbesserung der klinischen Qualität, der Sicherheit und des Risikos zusammenführt.

Grundlagen des Risikos

Organisationen des Gesundheitswesens verfolgen heute einen doppelten Ansatz beim Risikomanagement. Der eine basiert auf der Einhaltung von Vorschriften und bestimmt häufig die Strategie für die Informationssicherheit, während der andere auf klinische Ergebnisse und die Sicherheit der Patienten ausgerichtet ist.
Darüber hinaus ist die klinische Sicherheit auf die Bemühungen von Abteilungen wie Biomed oder Clinical Engineering abgestimmt, die mit der Wartung und Instandhaltung der Medizinprodukte betraut sind.

Dieser Unterschied wird in den Forschungsdaten deutlich, wenn wir danach fragen, wie das Risiko quantifiziert wird. In einigen Fällen wurde das Risiko in Bezug auf die Wartung von Software auf medizinischen Geräten formuliert, während es in anderen Fällen auf der Grundlage von

Segmentierung und eingesetzten Sicherheitskontrollen formuliert wurde. Bei fast allen Unternehmen war jedoch die Einhaltung von Vorschriften, die die Einführung von Sicherheitstechnologien vorantreiben, unterschiedlich stark ausgeprägt.

Ein Schlüsselelement, das alle Risikomanagementprogramme zu verbessern versuchen, ist die Priorisierung identifizierter Risiken mit Eintrittswahrscheinlichkeiten in Kombination mit der organisatorischen Toleranz und den Ressourcen zur Bewältigung der Auswirkungen. Da es in diesem Fall um IT- und Informationssicherheitsrisiken für das System geht, müssen geeignete Datenströme analysiert werden, die helfen, die Auswirkungen zwischen den Nuancen der Pflege und der Abhängigkeit von der Infrastruktur der Einrichtung zu unterscheiden, die erst kürzlich ihr digitales Selbst "gefunden" hat.

Da das Gesundheitswesen eine stark regulierte Branche ist, in der mehrere Arbeitsabläufe für verschiedene Arten von Risikobewertungen und entsprechende Vorschriften erforderlich sind, ist es wichtig, eine Standardisierung für risiko- und bedrohungsbezogene Datensätze zu nutzen, bevor diese als Input für Szenarien für das Notfallmanagement und die Geschäftskontinuitätsplanung verwendet werden. Dieser Datenstandard muss folgende Punkte berücksichtigen:

- Sicherheitsrisiko nach Behandlungsbereich oder Fachgebiet kontextualisiert
- Bedrohungsmodelle unter Berücksichtigung von IT-Hygiene und Privilegienmanagement
- Grundlegender Nutzungskontext für klinische und Gebäudemanagementsysteme
- Abhängigkeit von klinischen Anwendungen oder Hilfsanwendungen und/oder Anwendungsfälle für Dateninteroperabilität
- Workflow-Kontext für Abteilungen wie Biomed/Clinical Engineering und Facility Management

Bestrebungen wie das DSPT im Falle des NHS sind ein willkommener Schritt in die richtige Richtung.

Nutzung von sich überschneidenden Regelungen

So lästig dies auch klingen mag, können sich überschneidende Anforderungen in Vorschriften gleichzeitig mehrere Facetten einer Sicherheitsprogrammstrategie betreffen und die Kosten auf mehrere Finanzierungsquellen verteilen. Betrachten Sie das folgende Beispiel. In einer Umgebung des Gesundheitswesens gibt es Sicherheitsanforderungen, die sich aus den folgenden Punkten ergeben:

- Nationale / bundesstaatliche Gesetze und Vorschriften
- Gesetze und Vorschriften des Bundesstaates, der Provinz oder des Territoriums
- Informationssicherheitsstandards in Bezug auf
- Finanzielle Transaktionen
- Klinische Forschung und Datenzusammenarbeit
- Zusammenarbeit mit Verteidigungs- und Nachrichtendiensten

In jedem Fall kann ein Crosswalk-Ansatz entwickelt werden, der Unternehmen dabei hilft, die Nutzung geeigneter Standards zu priorisieren, um technologische Architekturen voranzutreiben und Betriebsdaten zu nutzen, die zur Erfüllung gesetzlicher Anforderungen abgeleitet wurden. Beispielsweise können die in PCI-DSS spezifizierten Sicherheitsanforderungen genutzt werden, um eine Segmentierung der Umgebung vorzunehmen, die dann für die Verwaltung von Gesundheitsdaten genutzt werden kann.

In einem anderen Anwendungsfall können Standards, die technische Ansätze für das Schwachstellenmanagement und die Risikopriorisierung durch die Zusammenarbeit mit klinischen Forschungsdaten vorschreiben, zur Verbesserung der Arbeitsabläufe im Sicherheitsbereich eingesetzt werden, deren Daten als Nachweis für die Einhaltung von Vorschriften auf staatlicher und nationaler

Ebene dienen können.

Diese Ideen sollen die Gestaltung von Prozessen erleichtern, die nicht nur auf die Einhaltung von Vorschriften ausgerichtet sind, sondern auch dazu dienen, die erforderlichen Aktivitäten so zu koordinieren, dass das Unternehmensrisiko mit der Belastbarkeit der klinischen Arbeitsabläufe in Einklang gebracht werden kann. Ein angemessener Zeitaufwand kann Organisationen dabei helfen, besser auf Vorfälle zu reagieren, die sich auf die Versorgung auswirken.

Realitäten der "Echtzeit"-Daten

Die Anforderungen an eine kontinuierliche Überwachung des Unternehmensrisikos erfordern ein Umdenken bei den Prozessen, die zur Ermittlung von Schwachstellen- und Auswirkungsdaten verwendet werden, und deren Umfang, der auf das Ökosystem der Gesundheitsgeräte abgestimmt ist. Die Daten aus unserer Untersuchung zeigen, dass die meisten Unternehmen zwar die Unterstützung der Führungsebene in Bezug auf diese Aktivitäten haben, die Umsetzung auf der operativen Ebene sich jedoch oft nur auf die Informationssicherheitsdaten und nicht auf die Gesamtheit der Auswirkungen von Medizinprodukten auf den klinischen Workflow konzentriert. Betrachtet man das Ökosystem der Medizinprodukte, so ist das Risikoprofil nicht bei allen Medizinprodukten gleich. Betrachten Sie die folgenden Beispiele:

- Geräte, die direkt für die Patientenversorgung eingesetzt werden (z. B. Infusionspumpen, Patientenmonitore)
- Hilfsgeräte zur Unterstützung der Pflege (z. B. Labor, Radiologie, sterile Verarbeitung)
- Betriebstechnologien mit kritischen Auswirkungen (z. B. Rohrpostsysteme, Wasser- und Sauerstoffmanagement, HVAC)
- Kontrollsysteme mit großen Auswirkungen auf den Betrieb (z. B. physische Sicherheit, Alarme, Aufzugskontrollsysteme)

All dies ist ein wesentlicher Bestandteil der "Sicherung der Patientenreise". Wenn Organisationen jedoch das Schwachstellenmanagement und ihre Ansätze zur Bewältigung des damit verbundenen Risikos in Bezug auf den klinischen Arbeitsablauf betrachten, sind die Ansätze immer noch zeitlich begrenzt. Sie müssen zu Prozessen übergehen, die eine Echtzeitanalyse von Schwachstellendaten und deren Auswirkungen auf betriebliche Arbeitsabläufe unterstützen.

Für den Übergang vom alten Ansatz zu einer Methodik des Schwachstellenmanagements im Stil der kontinuierlichen Überwachung können Unternehmen die in den alten Plattformen vorhandenen Funktionen nutzen und Innovationen mit neuen Ansätzen hinzufügen, die diese berücksichtigen:

- Netzwerkverhalten
- Kommunikationsmethodik (Peer-to-Peer/Luftraum, z. B. Bluetooth, Z-Wave)
- Passives ereignisbasiertes Scannen in Echtzeit vs. zeitgesteuertes Scannen
- Nutzungsdaten
- Baseline-Geräteverhaltenstelemetrie

Mit diesen Ansätzen kann eine Architektur geschaffen werden, die nicht nur den technologischen Fußabdruck, sondern auch die Auswirkungen auf die Arbeitsabläufe in einer betrieblichen Umgebung berücksichtigt. Dies ist für Organisationen des Gesundheitswesens von entscheidender Bedeutung, da Betriebsumgebungen wie Biomed / Clinical Engineering oft aus Geräten bestehen, die von 30 Jahre alte Laborüberwachungsgeräte bis hin zu den neuesten Bildgebungsmodalitäten.
Wenn die Betriebsteams die Rolle berücksichtigen, die die Betriebstechnologien (OT) in einer Gesundheitsumgebung spielen, wird deutlich, dass das Schwachstellenmanagement nicht mehr nur ein Sicherheits-Toolkit ist, sondern eine wesentliche Komponente der Kontinuität des Betriebs.

Anstrengungen zur Umgestaltung bestehender Sicherheitsprogramme und betrieblicher Praktiken erfordern jedoch Investitionen. Dies wurde anhand von Forschungsdaten des NHS deutlich, die die Fortschritte bei der Implementierung von Sicherheitskontrollen für die Geräteidentifizierung und -segmentierung aufzeigten. Die Wirksamkeit muss jedoch noch unter Beweis gestellt werden, was die Herausforderungen bei den operativen Fähigkeiten aufzeigt. Investitionen müssen nicht immer finanzieller Art sein. Bei Programmen, die sich auf die Sicherheit von Geräteökosystemen im Gesundheitswesen beziehen, muss ein erheblicher Schulungsaufwand betrieben werden, um der Einführung von Daten und Prozessen Rechnung zu tragen, die den traditionellen Sicherheitsteams fremd sind. Ein angemessener Rahmen für die Umsetzung der Strategie kann dabei helfen, die Ziele und Erfolgskriterien einzugrenzen, die als nachweisbare Artefakte für die Einhaltung der Vorschriften eingestuft werden und den ROI in Bezug auf die Widerstandsfähigkeit des Unternehmens aufzeigen.

Menschen und Geld

In den letzten zehn Jahren wurden Sicherheitsinitiativen für medizinische Geräte aufgrund ihrer Eigenschaften als Edge-Computing-Geräte von der IT-Abteilung durchgeführt. Infolgedessen mussten sich die Organisationen des Gesundheitswesens einige Zeit nehmen, um die betrieblichen Auswirkungen der Anwendung herkömmlicher Sicherheitsmethoden bei der Eindämmung von Bedrohungen zu verstehen, die sich auf die Pflege und die Patientensicherheit auswirken können. Dieser Ansatz hat zwar zu technologischen Innovationen geführt, aber wir müssen immer noch den Kontext der klinischen und betrieblichen Arbeitsabläufe berücksichtigen.

Warum die Trennung zwischen dem klinischen und dem operativen Bereich? Erstere konzentrieren sich auf die Bereitstellung von Pflegeleistungen, während letztere die “Sanitäranlagen” bereitstellen, die für den Erfolg der ersteren erforderlich sind. Dieser winzige Unterschied hat große Auswirkungen darauf, wie Unternehmen ihre Strategie anpassen müssen, wenn sie eine Sicherheitsinitiative für medizinische Geräte, OT oder industrielle Kontrollsysteme (ICS) einleiten.

Bei der Planung der Finanzierung ist es von entscheidender Bedeutung, den Umfang zu verstehen, da dies eine erste Ausrichtung auf den Zweck der Einführung des Programms schafft. Dies kann die Patientensicherheit oder das Risikomanagement bei erheblichem Wachstum oder die Vorbereitung auf eine Fusion oder Übernahme sein. In jedem Fall ist es sinnvoll, Finanzierungsquellen zu nutzen, die eng mit den Ergebnissen des “Warum” und nicht mit dem “Wie” (in diesem Fall der Technologie) verbunden sind.

Aus personeller Sicht sollte ein Ansatz entwickelt werden, der die bestehenden Mechanismen für das Risikomanagement und die Übernahme durch die Führung nutzt. Es wird ein gewisses Maß an Investitionen in Vollzeitäquivalente erforderlich sein, sei es organisch oder durch eine Partnerschaft mit einem Managed-Service-Anbieter. Diese müssen durch Fachwissen aus den klinischen, operativen und Risikoabteilungen ergänzt werden, damit vor dem Kauf der Technologie geeignete Funktionen für die Datenberichterstattung und Anwendungsfälle entwickelt werden können und eine Ausrichtung auf klinische und operative Anwendungsfälle möglich ist.

Unter Berücksichtigung menschlicher Faktoren und Arbeitsabläufe kann eine angemessene Schulung in den folgenden Bereichen die Leistungsfähigkeit der Teams für Informationssicherheit und klinische

Abläufe erheblich beeinflussen. Geeignete Testmethoden müssen implementiert werden, die Folgendes umfassen:

- Angleichung der Reaktion auf Sicherheitsvorfälle an die Notfallmaßnahmen und die klinischen Arbeitsabläufe
- Festlegung von Geschäftskontinuitätsmetriken für organisatorische Schwellenwerte für Datenverluste und die Dauer von Systemausfallzeiten
- Verständnis der Zeitschwellen für die Arbeitsabläufe des Personals (z. B. die Zeit, die ein Biomed-Techniker benötigt, um eine Pumpe auszutauschen, die Zeit, die ein IT-Techniker benötigt, um eine Betrachtungsstation für einen CT-Scanner auszutauschen, die Zeit, die benötigt wird, um einen Handscanner für die Medikamentenausgabe bereitzustellen, usw.)

Am wichtigsten ist, dass die Einbeziehung von Sicherheitsszenarien wie Ransomware und Angriffe auf die Lieferkette als Teil von Notfallmanagementübungen dazu führt, dass das Muskelgedächtnis von IT- und Informationssicherheitsmitarbeitern richtig entwickelt wird, und dass es hilft, echte Zeitschätzungen für die Reaktion auf Vorfälle und die Wiederherstellung zu erstellen.

Die Einsicht in die Gesamtheit des Ökosystems der medizinischen Geräte ist für den Erfolg jeder Sicherheitsstrategie für medizinische Geräte entscheidend. Sie ist auch das grundlegende Element einer effektiven Bedrohungsmodellierung. Sie bietet Sicherheitsteams die realistischste Sicht auf die Angriffsfläche, wenn sie Sicherheitsinformationen im Hinblick auf die Auswirkungen auf den Betrieb analysieren.

Priorisierung von Schwachstellen und Nutzung der Modellierung

Bedrohungsmodelle sind ein wesentlicher Bestandteil der Sicherheitsstrategie, da sie die folgenden Telemetriedaten für eine effiziente Reaktion liefern:

- Dynamische Sicht auf die Angriffsfläche
- Anfälligkeit und Sicherheitsrisiko im gesamten Ökosystem
- Identifizierung von Bedrohungsakteuren
- Ansicht der Angriffsvektoren
- Aufzählung der Vermögenswerte des Krankenhauses (Betrieb) im Vergleich zu den Patientenwerten (Klinik)
- SecOps-Fähigkeit
- Metriken zur Verknüpfung der betrieblichen Realität mit akademischen Daten zum wahrgenommenen Risiko

Diese Modelle ermöglichen es den Sicherheitsteams nicht nur, geeignete Arbeitsabläufe für die Reaktion auf Vorfälle zu entwerfen und zu testen, sondern sie dienen auch als Datenquelle für das Notfallmanagement, um Notfallprozesse zu testen und den Betrieb im Falle eines Vorfalls zu simulieren. In vielen Unternehmen wurden zwar erhebliche Fortschritte in dieser Hinsicht erzielt, aber es sind noch Investitionen erforderlich, um eine geeignete Testinfrastruktur zu konzipieren und zu implementieren, so dass tatsächliche Metriken zur Bestimmung des Betriebsrisikos verwendet werden können und nicht nur Daten, die aus Tabletop-Übungen stammen.

Ein Schlüsselelement der Bedrohungsmodellierung ist das Verständnis der Rolle, die das Schwachstellenmanagement nicht nur für die Identifizierung von Sicherheitsrisiken, sondern auch für potenzielle Auswirkungen auf die Sicherheit und den Betrieb in einer Gesundheitsumgebung spielt. Fortschritte in der Sicherheitstechnologie wie Armis ermöglichen es Organisationen des Gesundheitswesens nun, nicht nur das Bedrohungsprofil für ein bestimmtes Gerät in der Umgebung zu beschreiben, sondern auch zu analysieren:

- Einblick in vor- und nachgelagerte Datenflüsse
- Kontext für vorübergehende Geräte, die nicht mit dem Unternehmensnetz verbunden sind
- Gerätetelemetrie bei Nutzung von Luftraumtechnologien
- Einsicht in maßgeschneiderte Datenprotokolle des Gesundheitswesens als Teil des Behavioral Mapping

Diese Teile sind wichtig, da sie oft zu wichtigen Arbeitsabläufen und klinischen Zusammenhängen

führen, die bei der Priorisierung von Vorfällen benötigt werden, da sie dazu beitragen, Risiken für die Patientensicherheit, die Verfügbarkeit von Geräten und die Fähigkeit, die richtige Pflege zur richtigen Zeit zu leisten, zu artikulieren. Ein weiterer greifbarer Effekt dieses Ansatzes ist die betriebliche Effizienz. Da die Daten, die in die Risikopriorisierung einfließen, bereits mit der entsprechenden Relevanz in Bezug auf organisatorische Nuancen (sowohl aus technologischer als auch aus Workflow-Perspektive) kontextualisiert wurden, ist die Zuverlässigkeit der identifizierten Prioritäten ist hoch, was zu einer erheblichen Verkürzung der Reaktionszeiten auf Vorfälle und zu einem effizienteren Kostenmanagement in Bezug auf die Geräte- und Anlagenbestände führt.

Nutzungskontext zur Steuerung von Reaktions- und Wiederherstellungsprozessen

Aus klinischer Sicht muss die nächste Iteration der ROI einer Sicherheitsstrategie für medizinische Geräte den Blickwinkel von der traditionellen Hypothese der Sicherung angeschlossener medizinischer Geräte im stationären Umfeld erweitern. Das klinische Risikomanagement umfasst die folgenden Aspekte:

- Überwachung der klinischen Arbeitsabläufe im Einklang mit Qualitäts- und Sicherheitsstandards und -richtlinien
- Analyse der Gerätenutzung zur Minimierung der Auswirkungen auf die Patientenzufriedenheit (z. B. Wartezeiten)
- Effizienz klinischer Verfahren (z. B. Verringerung des übermäßigen Einsatzes einer bestimmten Art von Medikamenten)
- Sicherstellung der Integrität der für die klinische Entscheidungshilfe verwendeten Datenströme
- Alle oben genannten Tätigkeiten in jeder Art von Pflegeumgebung - stationär, ambulant, ferngesteuert usw.

In der Praxis ist es schwierig, diese zu berücksichtigen, wenn man die Gesamtheit der von einem Leistungserbringer erbrachten Leistungen betrachtet. Um dies zu verhindern, können Organisationen den Umfang nach Fachgebiet, Marktausrichtung, strategischen klinischen Initiativen, Compliance-Initiativen usw. eingrenzen, um die Alarmmüdigkeit zu minimieren und den Risiko-Governance-Prozess organisch und auf einem überschaubaren Kostenniveau wachsen zu lassen.

Die Konzentration der Bemühungen auf Echtzeitberichte und die Integration mit dem IT-Betrieb kann dazu beitragen, die Reaktionszeiten des Helpdesks zu verkürzen und die Effizienz der Analyse-Workflows zu steigern, um Betriebskosten zu sparen. Im biomedizinischen Bereich und in den Einrichtungen können diese Integrationen zur Rationalisierung der einrichtungsübergreifenden Wartungsabläufe beitragen und die Basiskosten für Verträge mit Drittanbietern von Gesundheitsdienstleistungen senken. Die Dateninteroperabilität ist von entscheidender Bedeutung, da sie den bidirektionalen Datenpfad zwischen der Sicherheitsarchitektur und den bestehenden Investitionen in Governance- und Risikomanagementplattformen herstellt, was zu zusätzlichen Betriebskosteneinsparungen führt.

SCHLUSSFOLGERUNG

Risikorahmen, Reaktionstaktiken und Bedrohungsmodelle sind ohne eine tatsächliche Testmethodik nur bedingt wirksam. Um die Auswirkungen dieser Angriffe zu verringern und die Reaktionsfähigkeit zu verbessern, gibt es keinen Ersatz für tatsächliche Simulationen und Tests von Workflow-Störungen oder Systemausfällen. Organisationen des Gesundheitswesens, die diesen Bemühungen im Rahmen des normalen Geschäftsbetriebs Priorität einräumen, können ihre Risikotelemetrie abwägen und Daten berücksichtigen, z. B. wie lange es dauerte, bis die Systeme wiederhergestellt waren, wie sich die "verschlechterte Leistung" auf die Benutzer auswirkte und ob die Partnerschaften für Ressourcen und Technologie wie vorgesehen funktionierten. Mit der Zeit können das Muskelgedächtnis und die aus diesen Übungen und Tests gewonnenen Erkenntnisse als Grundlage dienen, auf der die Widerstandsfähigkeit eines Unternehmens jeden Angriff auf seine Umgebung übersteht.
Armis hat sich verpflichtet, seinen Kunden im Gesundheitswesen bei der Verwirklichung der Vision zu helfen, dass Risikomanagement und Betriebskontinuität symbiotisch existieren können. Mit angemessenen Investitionen und einem bewussten Sinn für Dringlichkeit können wir die Informationssicherheit zu einer organischen Erweiterung des klinischen Risikomanagementprozesses machen.

"Für einen Großkonzern mag ein IT-Audit Routine sein und es geht letztendlich um Fine Tuning und die Anpassung an neue Gegebenheiten. Bei einem Start-up sieht die Situation ganz anders aus. Hier müssen Prozesse etabliert und Mitarbeiter sensibilisiert werden. Sodann braucht es eine Infrastruktur, die sich dem dynamischen Wachstum anpasst. Das Managed Services Angebot und die Security-Expertise von omniIT machen IT-Sicherheit auch für Start-ups finanzierbar.

Patryk Wlodarczyk
CEO omniIT

Über omniIT

Wir aktivieren Ihre digitale DNA!

Als Full-Service IT-Dienstleister erstreckt sich unser Angebot von IT-Sicherheit über die IT-Infrastruktur bis hin zur Software-Entwicklung, Beratungsprojekten und Managed IT-Services. Nutzen Sie uns als verlängerte Werkbank, um Ihre Ziele zeitnah und mit den erwarteten Ergebnissen zu erreichen.

Unser Team arbeitet für den Erfolg nationaler und internationaler Unternehmen - egal ob Mittelstand oder Großkonzern aus der Technologie-, Automobil-, Finanz- oder Telekommunikationsbranche. Wir agieren stets transparent und kommunizieren auf Augenhöhe.